UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

MARY MARTINEZ on behalf of herself and all others similarly situated, Plaintiff, v. THOMPSON COBURN LLP, and PRESBYTERIAN HEALTHCARE SERVICES, Defendants.	Case No. _____ **CLASS ACTION COMPLAINT** **DEMAND FOR A JURY TRIAL**

Plaintiff Mary Martinez ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendants Thompson Coburn, LLP ("Thompson") and Presbyterian Healthcare Services ("Presbyterian"), collectively ("Defendants") on behalf of herself and all others similarly situated, and alleges, upon information and belief, except as to her own actions, the investigation of counsel, and facts that are a matter of public record:

INTRODUCTION

1. This civil action pursues monetary damages as well as injunctive and declaratory relief from Defendants, stemming from their negligence in safeguarding specific Personally Identifiable Information ("PII") and Protected Health Information ("PHI").

2. Between May 28, 2024 and May 29, 2024, an unknown actor grained access Thompson's network systems, resulting in the unauthorized disclosure of the PII and PHI of Plaintiff and the Class Members (the "Data Breach"). Such information encompasses, but is not limited to, name, medical record number, patient account number, prescription/treatment information, clinical information, and medical provider information (collectively, "Private Information").

3. Thompson is a nationwide law firm with experience in data breach litigation with

its primary office in St. Louis, Missouri.[1]

4. Presbyterian is a healthcare provider that serves patients in New Mexico. Presbyterian provided Thompson with access to its patients' files in connection with receiving legal services.

5. Plaintiff and Class Members entrusted their sensitive personal information to the Defendants, with the mutual understanding that it would be protected against disclosure. However, due to the Data Breach, this information was targeted, compromised, and unlawfully accessed.

6. Defendants systematically collected and maintained specific Private Information of the Plaintiff and the putative Class Members (defined below). These individuals are current or former patients of Presbyterian and their Private Information includes protected health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

7. The Data Breach occurred because Defendants failed to implement reasonable security procedures and practices, failed to disclose material facts surrounding its deficient data security protocols, and failed to timely notify the victims of the Data Breach.

8. As a result of Defendants' failure to protect the sensitive information they were entrusted to safeguard, Plaintiff and Class Members did not receive the benefit of their bargain and now face a significant risk of medical-related identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest

[1] https://www.thompsoncoburn.com/services/practices/cybersecurity/litigation-and-data-breach (last accessed November 20, 2024).

and costs, and members of the proposed Class, including Plaintiff, are citizens of states different from Defendants.

10. This Court has jurisdiction over Thompson through its business operations in this District, the specific nature of which occurs in this District. Thompson's principal place of business is located within this District, indicating a deliberate engagement with the markets here. Consequently, the exercise of jurisdiction by this Court is not only justified but also appropriate, given Thompson's intentional involvement in this District's economic activities.

11. This Court has specific personal jurisdiction over Defendant Presbyterian because it purposefully availed itself to the laws of this District by providing its patients Private Information to Defendant Thompson in this District.

12. Venue is proper pursuant to 28 U.S.C. § 1391(a)(1) due to the Thompson's principal place of business being situated within this District. Moreover, a significant portion of the events and omissions that form the basis of this action transpired within this District. Hence, it is fitting that this Court serves as the venue for adjudicating this matter.

PARTIES

13. Mary Martinez is a resident and citizen of Albuquerque, New Mexico and has been a patient of Presbyterian Healthcare Services. Presbyterian obtained and stored Plaintiff's Private Information in connection with her treatment at Presbyterian Healthcare Services.

14. Defendant, Presbyterian Healthcare Services, is a New Mexico non-profit corporation with its principal place of business at 5921 San Mateo Blvd. NE, Albuquerque, NM.

15. Defendant, Thompson Coburn LLP, is a Missouri Corporation, with its principal place of business at One US Bank Plaza, Suite 2500, Saint Louis, MO 63101. Defendant can be served through its registered agent, Roman P. Wuller, at One US Bank Plaza, Suite 2700, St. Louis, MO 63101.

FACTUAL ALLEGATIONS

Defendants Knew the Risks of Storing Valuable Private Information and the Foreseeable Harm to Victims.

16. Thompson is a law firm that holds itself out as a nationwide full-service law firm with offices located in Brimingham, Chicago, Dallas, Los Angeles, New York, Southern Illinois, St. Louis and Washington, D.C. It represents that it uses "state-of-the-art technology."[2]

17. Thompson, as it represented to current and prospective clients, was well aware that "the consequences of failing to appropriately mitigate cyber vulnerabilities can be devastating."[3]

18. On information and belief, as part of its practice, Thompson collects and stores the Private Information of third-party patients from Presbyterian.

19. As a self-proclaimed expert in Data Privacy and Security and handling highly sensitive aspects of its clients' business, Thompson understood the need to protect its clients' patients' data and prioritize its data security.

20. Presbyterian is a hospital system located in New Mexico comprised of nine hospitals, a multi-specialty medical group with more than 900 providers and a statewide health plan. One in three New Mexicans are served by Presbyterian.[4] It is "New Mexico's largest private employer with over 13,000 employees."[5]

21. In its privacy policy, Presbyterian promises that it has "policies and procedures to protect the privacy of health information that [] identif[ies] you," including:

- "We have a training program to educate our employees and others about our privacy

[2] https://www.thompsoncoburn.com/firm (last visited November 21, 2024).
[3] https://www.thompsoncoburn.com/services/practices/cybersecurity (last visited November 21, 2024).
[4] https://www.phs.org/about-us (last visited November 21, 2024).
[5] https://www.fiercehealthcare.com/providers/unitypoint-health-presbyterian-healthcare-services-call-11b-merger#:~:text=For%20the%202022%20fiscal%20year,of%20his%20employees%20their%20jo (last visited November 21, 2024).

policies."

- "Your health information is only used or shared for our business purposes or as otherwise required or allowed by law."
- "When a service involving your health information is being performed by a third party, we require a written agreement with them to protect the privacy of your health information."
- "We are required by law to maintain the privacy of your health information."
- "We have a legal duty to notify you, and you have a right to know when your protected health information has been inappropriately accessed, used, or disclosed as a result of a breach."
- "We will not use or share your health information without your written authorization unless required by law."[6]

22. As part of the process of collecting Private Information from patients, including Plaintiff, Presbyterian pledged to ensure confidentiality and adequate security for the data it gathered from patients. This commitment was articulated through its relevant privacy policy, patient's rights handout, and other disclosures, adhering to statutory privacy requirements. Specifically, Presbyterian represented that Plaintiff and other patients have the right to "have confidentiality of your medical records and personal information."[7]

23. Plaintiff and the Class Members, as patients of Presbyterian, trusted these assurances and counted on this sophisticated business entity to maintain the confidentiality and security of their sensitive Private Information. They expected Presbyterian to use this information

[6] https://onbaseext.phs.org/PEL/DisplayDocument?ContentID=wcmprod1029971 (Last visited November 21, 2024).
[7] https://onbaseext.phs.org/PEL/DisplayDocument?ContentID=PEL_00182934 (last accessed November 21, 2024).

solely for business purposes and to make only authorized disclosures. Patients, in general, insist on security measures to protect their Private Information, particularly when it involves sensitive details.

24. Despite recognizing its duty to do so, on information and belief, Presbyterian has not implemented reasonable cybersecurity safeguards or policies to protect its patients' Private Information or supervised its IT or data security agents and employees, including Thompson, to prevent, detect, and stop breaches of its systems. As a result, Presbyterian left significant vulnerabilities in its use and storage of Plaintiff and the Class's Private Information for cybercriminals to exploit and gain access to patients' Private Information.

The Data Breach

25. Plaintiff is a patient of Presbyterian.

26. As a condition of receiving services from Presbyterian, Presbyterian requires its patients to disclose PII/PHI including but not limited to, their names, medical records numbers, patient account numbers, prescription/treatment information, clinical information, and medical provider information. Presbyterian used that PII/PHI to facilitate its business and provision of services to Plaintiff, and required Plaintiff to provide that PII/PHI to obtain services.

27. On information and belief, Presbyterian provided Thompson with Plaintiff's Private Information as part of the legal services Thompson provided to Presbyterian. Thus, Thompson was granted access and custody of Plaintiff's Private Information including but not limited to name, medical records number, patient account number, prescription/treatment information, clinical information, and medical provider information.

28. Defendants collect and maintain patients' sensitive Private Information in their computer systems.

29. In collecting and maintain the Private Information, Defendants agreed to safeguard the data using reasonable means according to their internal policies and federal law.

30. Thompson first detected suspicious activity on May 29, 2024. Following an internal investigation, Thompson discovered that between May 28, and May 29, 2024, a cyber-criminal viewed or took information stored within Thompson's systems.

31. Despite representing itself as cyber security experts, Thompson's own data security policies and systems were inadequate and permitted a cyber-criminal to compromise the files of hundreds of thousands of Presbyterian patients. Presbyterian failed to exercise sufficient due diligence in verifying and overseeing Thompson's data security policies and systems. By entrusting Thompson with patients' Private Information without proper oversight or ensuring robust safeguards, Presbyterian directly contributed to the data breach.

32. Thompson admits that the Private Information was actually accessed and exfiltrated, "certain information stored within our environment was viewed or taken by an unauthorized actor."

33. It was not until nearly 6 months later, November 6, 2024, that Defendants provided notice to Plaintiff and the Class that it had suffered a Data Breach.

34. Despite the lack of transparency about the root cause of the incident, the Notice reveals key facts: a) the Data Breach was perpetrated by cybercriminals; b) these cybercriminals initially breached Thompson's networks and systems, subsequently viewing or exfiltrating data; and c) within Thompson's networks and systems, the cybercriminals specifically targeted information, potentially including Plaintiff's and Class Members' Private Information and other sensitive data for download and theft.

35. The Notice provided by Thompson is critically deficient, failing to provide critical information about the Data Breach. For example, the Notice omits when the sensitive Private Information was taken by the unauthorized party, when Thompson "launched an investigation," the full extent of the data accessed or exposed, when Thompson took action to stop the breach, whether

the breach has been fully remediated, and how Thompson confirmed what information was accessed.

36. Defendants provide no explanation for why they let the Private Information of Plaintiff and Class Members sit in the hands of the criminal hackers for nearly six months after they detected the breach before attempting to notify affected patients.

37. By waiting to disclose the Data Breach and by downplaying the risk that victims' Private Information would be misused by criminals, Defendants prevented victims from taking meaningful, proactive, and targeted mitigation measures to protect themselves from harm.

Preventable Data Breaches: Safeguarding Against Unnecessary Compromises

38. Defendants neglected to employ adequate security procedures and practices suitable for the sensitive nature of the information entrusted to them by Plaintiff and Class Members. This failure resulted in the exposure of Private Information, highlighting a lack of measures such as encryption or timely deletion when the information was no longer necessary.

39. Defendants could have averted this Data Breach by taking necessary precautions such as appropriately encrypting or implementing robust protection measures for their equipment and computer files containing Private Information.

40. As stated by the Federal Bureau of Investigation, "[P]revention is the most effective defense against ransomware, and it is crucial to implement precautionary measures for protection."[8]

41. To effectively prevent and detect cyber-attacks and ransomware incidents, the Defendant could have implemented the following measures, as recommended by the United States Government:

- Awareness and Training Program: Develop and implement a comprehensive awareness

[8] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited November 22, 2024).

and training program to educate employees and individuals about the threat of ransomware and how it is typically delivered.

- Strong Spam Filters: Enable robust spam filters to block phishing emails from reaching end users. Utilize technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to authenticate inbound email and prevent email spoofing.

- Email Scanning: Scan all incoming and outgoing emails to detect threats and filter out executable files from reaching end users.

- Firewall Configuration: Configure firewalls to block access to known malicious IP addresses.

- Patch Management: Regularly patch operating systems, software, and firmware on devices. Consider implementing a centralized patch management system for efficiency.

- Anti-virus and Anti-malware Programs: Set up anti-virus and anti-malware programs to conduct automatic regular scans.

- Privileged Account Management: Manage privileged accounts based on the principle of least privilege, restricting administrative access only to those who absolutely require it and limiting usage to necessary situations.

- Access Controls: Configure access controls, including file, directory, and network share permissions, with the principle of least privilege in mind.

- Macro Script Disabling: Disable macro scripts from office files transmitted via email. Consider using Office Viewer software for opening Microsoft Office files transmitted via email instead of full office suite applications.

- Software Restriction Policies (SRP): Implement SRP or similar controls to prevent programs from executing from common ransomware locations.

- Remote Desktop Protocol (RDP) Disablement: Consider disabling Remote Desktop Protocol (RDP) if it is not in active use.

- Application Whitelisting: Utilize application whitelisting to only allow systems to execute programs that are known and permitted by security policy.

- Virtualized Environment Execution: Execute operating system environments or specific programs in a virtualized environment to enhance security.

- Data Categorization and Separation: Categorize data based on organizational value and implement both physical and logical separation of networks and data for different

organizational units.[9]

42. To effectively prevent and detect cyber-attacks or ransomware incidents, Defendants could have implemented the following measures, as recommended by the Microsoft Threat Protection Intelligence Team:

> **Secure Internet-Facing Assets**
>
> Apply latest security updates
> Use threat and vulnerability management
> Perform regular audit; remove privileged credentials;
>
> **Thoroughly investigate and remediate alerts**
>
> Prioritize and treat commodity malware infections as potential full compromise;
>
> **Include IT Pros in security discussions**
>
> Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> **Build credential hygiene**
>
> Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
>
> **Apply principle of least-privilege**
>
> Monitor for adversarial activities
> Hunt for brute force attempts
> Monitor for cleanup of Event Logs
> Analyze logon events;
>
> **Harden infrastructure**
>
> Use Windows Defender Firewall
> Enable tamper protection
> Enable cloud-delivered protection
> Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[10]

43. Considering that Defendants were entrusted with storing the Private Information of

[9] *Id.* at 3-4.
[10] *See* Human-operated ransomware attacks: A preventable disaster (Mar. 5, 2020), *available at:* https://www.microsoft.com/en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/(last accessed November 21, 2024).

both current and former patients, it was imperative for them to implement all of the aforementioned measures to effectively prevent and detect cyberattacks.

44. The Data Breach underscores Defendants' failure to sufficiently implement one or more of the aforementioned measures aimed at preventing cyberattacks. This lapse led to the Data Breach, enabling data thieves to access and acquire the Private Information of, according to available information, thousands to tens of thousands of individuals, including Plaintiff and Class Members.

Defendants' Acquisition, Collection, and Storage of Patients' Private Information

45. Presbyterian accumulates, gathers, and maintains an extensive volume of Private Information concerning both its present and past patients.

46. As a prerequisite for becoming a patient of Presbyterian or purchasing medical supplies from the organization, Presbyterian mandates that patients and other individuals entrust it with highly sensitive personal information.

47. By acquiring, gathering, and utilizing the Private Information of Plaintiff and Class Members, Presbyterian undertook legal and equitable obligations. It was well aware, or should have been, of its responsibility to safeguard Plaintiff's and Class Members' Private Information from unauthorized disclosure.

48. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Presbyterian absent a promise to safeguard that information.

49. Upon information and belief, during the process of collecting Private Information from patients, including Plaintiff, Presbyterian purportedly pledged to ensure confidentiality and sufficient security for their data. This commitment was purportedly articulated through its relevant privacy policy and other disclosures, in adherence to statutory privacy mandates.

50. Certainly, on its website, Presbyterian assures that the Site is equipped with security

measures to prevent loss, misuse, or alteration of information within their purview.

51. Plaintiff and the Class Members placed their trust in Defendant to uphold the confidentiality and secure maintenance of their Private Information, to utilize this data solely for business purposes, and to make authorized disclosures of this information only.

Defendants' Awareness of Cybersecurity Risks in Healthcare Entities Handling Private Information

52. Given the significant rise in cyber-attacks and data breaches targeting healthcare entities responsible for collecting and storing Private Information, such as Defendants, prior to the breach date, Presbyterian's data security obligations were of paramount importance.

53. Data breaches, including those directed at healthcare and healthcare adjacent entities housing Private Information within their systems, have proliferated extensively.

54. In the third quarter of the 2023 fiscal year alone, 733 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[11]

55. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including Change Healthcare (potentially hundreds of millions of patients, March 2024), HCA Healthcare (11-million patients, July 2023), Managed Care of North America (8-million patients, March 2023), PharMerica Corporation (5-million patients, March 2023), HealthEC LLC (4-million patients, July 2023), ESO Solutions, Inc. (2.7-million patients, September 2023), Prospect Medical Holdings, Inc. (1.3-million patients, July-August 2023), Defendants knew or should have known that its electronic records would be targeted by cybercriminals.

56. Certainly, cyber-attacks, have garnered such notoriety that both the Federal Bureau of Investigation and the U.S. Secret Service have issued warnings to potential targets, aiming to alert them and fortify their readiness against potential attacks. As elaborated in one report, smaller entities

[11] *See* https://www.idtheftcenter.org/wp-content/uploads/2023/10/20231011_Q3-2023-Data-Breach-Analysis.pdf (last accessed November 21, 2024).

tasked with storing Private Information are particularly appealing to ransomware criminals due to their typically weaker IT defenses and strong incentive to swiftly regain access to their data.[12]

57. Moreover, as businesses increasingly rely on computer systems to conduct their operations, for instance, through remote work necessitated by the Covid-19 pandemic, and the proliferation of the Internet of Things (IoT), the threat posed by cybercriminals is amplified. This underscores the imperative for implementing sufficient administrative, physical, and technical safeguards.[13]

58. Defendants were well aware that unprotected or exposed Private Information, held by health and health adjacent companies like themselves, holds significant value and is highly coveted by malicious third parties aiming to unlawfully profit from such information through unauthorized access.

59. Defendants were aware, or reasonably should have been aware, of the criticality of safeguarding the Private Information belonging to Plaintiff and Class Members. Moreover, they were cognizant of the foreseeable repercussions in the event of a breach in its data security system, notably the substantial costs that would burden Plaintiff and Class Members as a consequence of such a breach.

60. Plaintiff and Class Members are now confronted with enduring years of persistent monitoring of their financial and personal records, along with a loss of privacy rights. This ongoing surveillance inflicts and will persist in causing significant damages to the Class, compounded by the potential fraudulent exploitation of their Private Information.

61. The injuries to Plaintiff and Class Members were directly and proximately caused by

[12] https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last accessed November 21, 2024).
[13] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last accessed November 21, 2024).

Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

62. The consequences stemming from Defendants' failures to secure the Private Information of Plaintiff and Class Members are enduring and profound. Following the theft of Private Information, the potential for fraudulent exploitation and the resultant harm to victims can persist for years.

63. As healthcare and healthcare adjacent entities responsible for safeguarding the Private Information of patients, Defendants were fully aware, or should have been, of the criticality of protecting the Private Information entrusted to it by Plaintiff and Class Members. Moreover, Defendants should have recognized the foreseeable consequences should their data security systems be breached, including the substantial costs imposed on Plaintiff and Class Members. However, Defendants failed to implement sufficient cybersecurity measures to avert the Data Breach.

Value of Private Information

64. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[15]

65. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity

[14] 17 C.F.R. § 248.201 (2013).
[15] *Id.*

credentials.[16]

66. Personal Information can be sold at a price ranging from $40 to $200 or even higher.[17]

67. Furthermore, Social Security numbers represent one of the most detrimental forms of Private Information to have stolen. This is due to the multitude of fraudulent purposes to which they may be put, and the significant challenge individuals face in altering them.

68. As per the Social Security Administration, whenever an individual's Social Security number is compromised, the risk of unauthorized access to various sensitive records escalates. This includes bank accounts, credit cards, driving records, tax and employment histories, and other private information. Furthermore, since many organizations still rely on Social Security numbers as the primary identifier, the exposure to identity theft and fraud persists.

69. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[18]

---

[16] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at:* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed November 21, 2024).

[17] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at:* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 21, 2024); (Criminals can also purchase access to entire company data breaches from $900 to $4,500) https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed November 22, 2024).

[18] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed November 22, 2024).

70. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[19]

71. Additionally, altering or invalidating a stolen Social Security number is a complex process. An individual cannot acquire a new Social Security number without substantial paperwork and evidence demonstrating actual misuse. In essence, preemptive measures to safeguard against potential misuse of a Social Security number are not feasible; an individual must provide evidence of ongoing fraudulent activity to qualify for a new number.

72. However, obtaining a new Social Security number may not necessarily resolve the issue. Julie Ferguson from the Identity Theft Resource Center explains that credit bureaus and banks can swiftly link the new number to the old one, resulting in the transfer of all previous negative information to the new Social Security number. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft.[20]

73. Theft of PHI, which was compromised in the Data Breach, is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with

---

[19] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/ (last accessed November 22, 2024).

[20] *Portier v. NEO Tech. Sols.*, No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc.*, 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiffs' Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] Social Security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target her in fraudulent schemes and identity theft attacks.").

yours, your treatment, insurance and payment records, and credit report may be affected."[21]

74. The increased efficiency of electronic health records introduces the risk of privacy breaches. These records contain a wealth of sensitive information, including patient data, diagnoses, lab results, medications, prescriptions, and treatment plans, all of which are highly valuable to cybercriminals. A single patient's comprehensive record can fetch hundreds of dollars on the dark web. Consequently, PHI and PII have become sought-after commodities, fueling a thriving "cyber black market" where criminals openly trade stolen payment card numbers, Social Security numbers, and other personal data on various underground internet platforms.

75. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[22] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[23] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[24] According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[25]

76. According to Pam Dixon, executive director of World Privacy Forum, medical identity theft is an escalating and perilous crime that severely limits its victims' options for recovery. Victims often endure financial consequences, and, even more distressingly, they frequently encounter

---

[21] *Medical I.D. Theft*, EFraudPrevention, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected (last accessed November 21, 2024).
[22] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed November 21, 2024).
[23] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed November 21, 2024).
[24] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed November 21, 2024).
[25] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://news.sophos.com/en-us/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/ (last accessed November 21, 2024).

inaccuracies added to their personal medical records as a result of the thief's actions.[26]

77. A study conducted by Experian revealed that the average cost of medical identity theft per incident is approximately $20,000. Additionally, the majority of victims of medical identity theft are compelled to cover out-of-pocket expenses for healthcare services they did not receive in order to reinstate their coverage. Furthermore, almost half of medical identity theft victims lose their healthcare coverage following the incident, while nearly one-third experience an increase in insurance premiums. Alarmingly, 40 percent of victims are unable to fully resolve their identity theft ordeal.[27]

78. Given the foregoing, the information compromised in the Data Breach holds far greater value compared to the loss of credit card information in a retailer data breach. In the latter scenario, victims have the option to cancel or close their credit and debit card accounts. However, the information compromised in this Data Breach cannot be simply "closed" and is exceedingly challenging, if not impossible, to alter.

79. In addition to other forms of fraud, identity thieves may fraudulently acquire driver's licenses, government benefits, medical services, and housing, or even provide false information to law enforcement.

80. The fraudulent activity stemming from the Data Breach might remain undetected for an extended period, possibly years. There can be a considerable delay between the occurrence of harm and its detection, as well as between the theft of Private Information and its utilization. This was highlighted in a study conducted by the U.S. Government Accountability Office (GAO) on data breaches:

---

[26] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed November 21, 2024).
[27] *Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed November 21, 2024).

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[28]

81. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Defendants' Noncompliance with FTC Guidelines

82. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

83. In 2016, the FTC revised its publication, "Protecting Personal Information: A Guide for Business," which outlined cybersecurity guidelines for businesses. These guidelines emphasize the importance of safeguarding personal patient information, appropriately disposing of unnecessary personal information, encrypting information stored on computer networks, comprehending network vulnerabilities, and implementing policies to address any security issues.[29]

84. The guidelines also advocate for businesses to employ an intrusion detection system to promptly detect breaches as they happen, monitor all incoming traffic for signs of attempted system hacking, be vigilant for unusually large data transmissions from the system, and have a prepared response plan in place in the event of a breach.[30]

85. Furthermore, the FTC advises companies to refrain from retaining Private

---

[28] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed November 22, 2024).
[29] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed November 22, 2024).
[30] *Id.*

Information for longer than necessary for transaction authorization, restrict access to sensitive data, mandate the use of complex passwords on networks, employ industry-proven security methods, monitor the network for any suspicious activity, and verify that third-party service providers have adopted reasonable security measures.

86. The FTC has taken enforcement actions against businesses for inadequately safeguarding patient data, considering the failure to implement reasonable and appropriate measures to prevent unauthorized access to confidential patient data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions provide additional clarification on the steps businesses must take to fulfill their data security obligations.

87. These FTC enforcement actions include actions against healthcare providers and healthcare adjacent companies like Defendants. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (Henry Ford) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

88. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, for failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

89. Defendants failed to properly implement basic data security practices.

90. Defendants failed to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information of their patients or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15

U.S.C. § 45.

91. Upon information and belief, Defendants were at all times fully aware of their obligations to protect the Private Information of their patients, Defendants were also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendants Noncompliance with HIPAA Guidelines

92. Presbyterian is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

93. Presbyterian is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[37] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

94. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

95. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

96. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

97. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

98. HIPAA's Security Rule mandates that Presbyterian:

a. Safeguard the confidentiality, integrity, and availability of all electronic protected health information created, received, maintained, or transmitted by the covered entity or business associate;

b. Shield against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Guard against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

99. HIPAA further requires Presbyterian to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

100. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

101. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires

Presbyterian to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[31]

102. HIPAA requires a covered entity to have and apply appropriate sanctions against patients of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

103. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

104. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e- and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[39] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-." US Department of Health & Human Services, Guidance on Risk Analysis.[32]

[31] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last accessed November 21, 2024).
[32] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed November 21, 2024).

Defendants' Noncompliance with Industry Standards

105. Experts in cybersecurity frequently highlight healthcare entities as particularly vulnerable to cyberattacks due to the high value of the Private Information they collect and maintain.

106. Several best practices have been identified that, at a minimum, should be implemented by healthcare and healthcare adjacent entities in possession of Private Information, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

107. Standard cybersecurity practices for healthcare and healthcare adjacent entities include installing robust malware detection software, monitoring and limiting network ports, securing web browsers and email systems, setting up firewalls, switches, and routers, and ensuring physical security systems are protected. Additionally, it is essential to safeguard communication systems and train staff on critical security protocols. Defendants failed to adhere to these best practices, including neglecting to properly train staff.

108. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

109. The aforementioned frameworks represent established industry standards for healthcare and healthcare adjacent entities. Based on available information, Defendants failed to

comply with one or more of these accepted standards, thereby allowing the threat actor to exploit vulnerabilities and cause the data breach.

Common Injuries

110. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the hands of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent. Consequently, Plaintiff and Class Members have sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) unconsented disclosure of their Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the effects of the Data Breach; (v) loss of benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and increased risk to their Private Information, which remains unencrypted and accessible to unauthorized third parties and is still backed up in Defendants' possession, subject to further unauthorized disclosures unless Defendants implement appropriate and adequate protective measures.

Data Breaches Heighten Victims' Risk of Identity Theft

111. The unencrypted Private Information of Class Members is highly likely to be sold on underground markets or offered for sale on the dark web, as this is the common *modus operandi* of hackers.

112. Unencrypted Private Information can also be obtained by companies that use it for targeted marketing without the consent of the Plaintiff and Class Members. In essence, unauthorized individuals can easily access the Private Information of the Plaintiff and Class Members.

113. The connection between a data breach and the risk of identity theft is straightforward and well-established. Criminals acquire Private Information to monetize it, often by selling the stolen data on the black market. Other criminals then purchase this information to commit

various identity theft-related crimes, as discussed below.

114. Plaintiff's and Class Members' Private Information holds significant value for hackers and cyber criminals. The data stolen in the Data Breach has been, and will continue to be, used in various malicious ways, allowing criminals to exploit Plaintiff and Class Members and profit from their misfortune.

115. Recognizing the dangers posed by the exposure of Social Security numbers, state legislatures have implemented laws to mitigate these risks. Social Security numbers can be exploited for fraudulent activities and to obtain sensitive personal, financial, medical, and familial information, potentially causing significant harm to individuals. Initially intended for federal Social Security System administration, these numbers have since become widely used for identity verification purposes.

116. Despite the risk of fraud associated with the theft of Social Security numbers, "just five of the nation's largest 25 banks have stopped using the numbers to verify a patient's identity after the initial account setup[.]"[33] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account."

117. One such example of criminals piecing together bits and pieces of compromised

[33] *See* https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/ (last accessed November 21, 2024).

Private Information for profit is the development of "Fullz" packages.[34]

118. Through "Fullz" packages, cyber-criminals can merge two sources of Private Information, combining unregulated data available elsewhere with criminally obtained data. This process results in remarkably comprehensive and accurate dossiers on individuals.

119. The emergence of "Fullz" packages indicates that the stolen Private Information from the Data Breach can readily be matched with Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. Essentially, even if specific details like emails, phone numbers, or credit card numbers were not part of the exfiltrated Private Information in the Data Breach, criminals can effortlessly compile a Fullz package and repeatedly sell it at inflated prices to unethical operators and criminal entities (like illicit telemarketers and scammers).

120. The presence and widespread availability of "Fullz" packages indicate that the Private Information pilfered from the data breach can effortlessly be correlated with the unregulated data, such as insurance information, belonging to the Plaintiff and other Class Members.

121. Consequently, even if specific details like insurance information were not compromised in the data breach, criminals can still effortlessly compile a comprehensive "Fullz" package. This detailed dossier can then be sold—and continually resold—to dishonest operators and other criminals, including illegal and fraudulent telemarketers.

[34] Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/), (last accessed November 21, 2024).

Mitigating Risk: Time Lost in Preventing Identity Theft and Fraud

122. In light of the acknowledged threat of identity theft, when a Data Breach transpires, and an individual receives notification from a company regarding the compromise of their Private Information, as in this instance, it is reasonable to anticipate that they will take measures and dedicate time to address the perilous scenario. This entails educating themselves about the breach and undertaking actions to minimize the risk of falling victim to identity theft or fraud. Neglecting to allocate time to review accounts or credit reports could potentially exacerbate financial harm. However, the valuable resource and asset of time are squandered in this process.

123. Plaintiff and Class Members have already devoted significant time to, and will continue to invest time in the future, undertaking various prudent measures. These include researching and validating the authenticity of the Data Breach and diligently monitoring their financial accounts for any signs of suspicious activity, which could potentially take years to uncover. Consequently, the Data Breach has inflicted tangible harm on Plaintiff and Class Members in the form of irreplaceable lost time dedicated to mitigation efforts.

124. Plaintiff's actions to mitigate the situation align with findings from the U.S. Government Accountability Office, as outlined in a 2007 report on data breaches. The report highlighted that individuals affected by identity theft encounter significant expenses and invest considerable time in rectifying damage to their reputation and credit history.[35]

125. Plaintiff's efforts to mitigate the situation align with the recommendations provided by the FTC for individuals affected by data breaches. These steps include contacting one of the credit bureaus to place a fraud alert (with consideration for an extended fraud alert lasting up to seven years

[35] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed November 21, 2024).

if identity theft occurs), reviewing credit reports, contacting companies to dispute fraudulent charges, implementing a credit freeze, and rectifying inaccuracies on credit report.[36]

Unconsented Disclosure of Private Information

126. PII and PHI constitute valuable property rights.[37] Sensitive PII can fetch prices as high as $363 per record, as reported by the Infosec Institute. Additionally, there exists a thriving legitimate marketplace for PII. In 2019 alone, the data brokering industry was estimated to be valued at around $200 billion.[38]

127. The data marketplace has reached a level of sophistication where patients have the option to directly sell their non-public information to a data broker. Subsequently, these brokers aggregate the data and furnish it to marketers or app developers.

128. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[39]

129. Theft of PHI carries significant consequences. A thief could potentially exploit your identity or health insurance details to seek medical treatment, obtain prescription medications, submit claims to your insurance provider, or access other healthcare services. If the thief's health information becomes intertwined with data breach victim's, it could impact victim's medical treatment, insurance coverage, payment records, and even victim's credit report.

130. The Data Breach has led to the compromise and unauthorized release of Plaintiff's

---

[36] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed November 21, 2024).

[37] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p.2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

[38] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed November 21, 2024).

[39] https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed November 21, 2024).

and Class Members' Private Information, which holds inherent market value in both legitimate and illicit markets. This unauthorized transfer of value occurred without any compensation provided to Plaintiff or Class Members for their property, resulting in an economic loss. Furthermore, the Private Information is now easily accessible, and its exclusivity has been lost, leading to further devaluation.

131. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security system were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

132. The fraudulent activity resulting from the Data Breach may not come to light for years.

133. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

134. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to, upon information and belief, thousands to tens of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

135. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

136. Considering the nature of the targeted attack in this case, involving sophisticated criminal activity and the sensitive Private Information at stake, there is a high likelihood that entire

datasets of stolen information have either been or will be circulated on the black market or dark web. Criminals intend to exploit this Private Information for identity theft crimes, such as opening bank accounts in victims' names for purchases or money laundering, filing fraudulent tax returns, securing loans or lines of credit, or submitting false unemployment claims.

137. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for insurance or unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

138. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

139. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of The Bargain

140. Furthermore, Defendants' poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Presbyterian and/or its agents for the provision of medical services, Plaintiff and other reasonable patients understood and expected that they were, in part, paying for the services and necessary data security to protect the Private Information, when in fact, Presbyterian did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Presbyterian.

Plaintiff Mary Martinez's Experience

141. Plaintiff Mary Martinez is a current patient of Presbyterian.

142. She was required to provide her Private Information to Presbyterian as a condition to receiving medical services at Presbyterian.

143. She received HIPAA and Privacy Notices from Presbyterian as part of receiving medical treatment.

144. Upon information and belief, at the time of the Data Breach, Presbyterian maintained Plaintiff's Private Information in its system.

145. In response to the Data Breach, Plaintiff diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and monitoring of financial accounts for any suspicious transactions, which may remain undetected for years.

146. Plaintiff has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, encompassing but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of her Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of her Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within the Defendants' possession, subject to further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

147. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

148. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

149. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

150. Plaintiff Martinez has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

151. Pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All citizens and residents of the United States whose Private Information was accessed and/or obtained by an unauthorized entity following the data breach disclosed by the Defendant Thompson in or around May 2024 (the "Class").**

152. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family patients.

153. Plaintiff reserves the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

154. Numerosity: The patients of the Class are so numerous that joinder of all patients is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of Defendants, upon information and belief, thousands of individuals were impacted. The Class is apparently identifiable within Defendants' records, and Defendants have already identified these individuals (as evidenced by sending them

breach notification letters).

155. Commonality: Common questions of law and fact exist as to all patients of the Class and predominate over any questions affecting solely individual patients of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class Members, including the following:

a. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendants had respective duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory

damages, and/or nominal damages as a result of Defendants' wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

156. Typicality: Plaintiff's claims are typical of those of the other patients of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other patient of the Class.

157. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

158. Adequacy: The Plaintiff will serve as a fair and effective representative for the Class Members, possessing no conflicting interests that would hinder the protection of their rights. The relief sought by the Plaintiff aligns with the collective interests of the Class, without any adverse implications for its members. The infringements upon the Plaintiff's rights and the damages incurred are emblematic of those experienced by other Class Members. Moreover, the Plaintiff has engaged legal counsel adept in navigating intricate class action and data breach litigation, demonstrating a commitment to vigorously pursue this case.

159. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously,

efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

160. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

161. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

162. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

163. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may

continue to act unlawfully as set forth in this Complaint.

164. Further, Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

165. Similarly, specific issues outlined in Rule 42(d)(1) warrant certification as they entail distinct yet shared concerns pivotal to advancing the resolution of this case and the interests of all parties involved. These issues include, but are not confined to:

a. Whether the Defendants failed to promptly notify both the Plaintiff and the class about the Data Breach;

b. Whether the Defendants bore a legal responsibility to exercise due diligence in the acquisition, storage, and protection of Private Information belonging to the Plaintiff and the Class;

c. Whether the security measures implemented by Defendants to safeguard their data systems aligned with industry best practices endorsed by data security experts;

d. Whether Defendants' omission of adequate protective security measures amounted to negligence;

e. Whether Defendants neglected to undertake commercially reasonable measures to secure patient Private Information; and

f. Whether adherence to data security recommendations outlined by the FTC and those advocated by data security experts could have feasibly prevented the occurrence of the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Class against Defendants)

166. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

167. Presbyterian requires its patients, including the Plaintiff and Class Members, to submit confidential Private Information as part of the standard process for receiving healthcare services. As such, Presbyterian owed Plaintiff and Class Members a non-delegable duty to protect the Private Information it collects.

168. This duty arose under common law, state and federal regulations, and Presbyterian's own policies, which promised to safeguard patient data from unauthorized access or disclosure. By collecting, maintaining, and sharing Plaintiff's Private Information as part of its healthcare operations, Presbyterian assumed a legal and ethical obligation to protect such sensitive data.

169. Presbyterian's duty also included the obligation to: (a) implement reasonable security practices and safeguards consistent with industry standards; (b) conduct adequate due diligence before entrusting third parties, such as Thompson, with Private Information; and (c) supervise and ensure that third parties adhered to the same rigorous standards for safeguarding Private Information.

170. Thompson voluntarily undertook a duty to protect Plaintiff's and Class Members' Private Information when it accepted access to and custody of this sensitive data from Presbyterian. By doing so, Thompson assumed a responsibility to maintain reasonable security measures to prevent unauthorized access, theft, or misuse of the information.

171. This duty arose from Thompson's business operations, its acceptance of the sensitive records, and applicable legal and ethical obligations, including the understanding that it was

responsible for safeguarding the entrusted Private Information consistent with industry standards and best practices.

172. Defendants breached their duties under the FTC Act, HIPAA, and other relevant standards, demonstrating negligence by failing to implement reasonable measures to protect Class Members' Private Information. Specific negligent actions and oversights by the Defendants include, but are not limited to:

173. Presbyterian breached its duty to protect Plaintiff's and Class Members' Private Information by:

a. Failing to adequately vet Thompson's data security protocols and capabilities before entrusting it with Private Information.

b. Failing to supervise Thompson's handling of sensitive Private Information, despite knowing or having reason to know of the risks associated with sharing patient data with third parties.

c. Failing to ensure Thompson maintained industry-standard security systems, protocols, and practices to protect the Private Information in its possession before sharing it with Thompson.

d. Transferring sensitive Private Information without sufficient oversight mechanisms to ensure its protection.

e. Neglecting to remove Private Information of former patients that was no longer required to be retained according to regulations.

174. Likewise, Thompson breached its duty to protect Plaintiff's and Class Members' Private Information by:

a. Neglecting to adopt, implement, and maintain sufficient security measures to safeguard Class Members' Private Information.

b. Inadequately monitoring the security of its networks and systems.

c. Allowing unauthorized access to Class Members' Private Information.

d. Failing to promptly detect that Class Members' Private Information had been compromised.

e. Failing to promptly and adequately inform Class Members about the occurrence and extent of the Data Breach, preventing them from taking appropriate measures to mitigate the risk of identity theft and other damages.

175. Defendants' duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship.

176. Defendants knew or should have known that Private Information, particularly within the healthcare and legal services contexts, is a prime target for cybercriminals. The sensitive nature of this data and its value on the black market made Plaintiff and Class Members part of a foreseeable, high-risk group that would suffer harm if their Private Information was not adequately protected.

177. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

178. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

179. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) the unconsented disclosure of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

180. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

181. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class against Defendants)

182. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

183. According to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants were obligated to furnish fair and adequate computer systems and data security practices to protect the private information of both the Plaintiff and Class Members.

184. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

185. Defendants breached their duties to Plaintiff and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

186. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se.*

187. Plaintiff and Class Members are within the class of persons the statutes were intended to protect and the harm to Plaintiff and Class Members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

188. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

189. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that by failing to meet their duties, Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

190. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to nominal, compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach Of Implied Contract
(On Behalf of Plaintiff and the Class against Defendant Presbyterian)

191. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

192. Plaintiff and Class Members were required to deliver their Private Information to Presbyterian as part of the process of obtaining services at Presbyterian. Plaintiff and Class Members paid money, or money was paid on their behalf, to Presbyterian in exchange for services.

193. Presbyterian solicited, offered, and invited Class Members to provide their private information as part of its regular business practices. The Plaintiff and Class Members accepted Presbyterian's request and provided their private information to Defendants.

194. Presbyterian solicited, offered, and invited Class Members to provide their private information as part of its regular business practices. The Plaintiff and Class Members accepted Presbyterian's request and provided their Private Information to Presbyterian solicited, offered, and invited Class Members to provide their private information as part of its regular business practices.

195. Plaintiff and the Class entrusted their Private Information to Presbyterian. In so doing, Plaintiff and the Class entered into implied contracts with Presbyterian by which Presbyterian agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

196. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Presbyterian's data security practices complied with relevant laws and regulations (including HIPAA and FTC guidelines on data security) and were consistent with industry standards.

197. Implicit in the agreement between Plaintiff and Class Members and Defendants to

provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

198. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Presbyterian, on the other, is demonstrated by their conduct and course of dealing.

199. On information and belief, at all relevant times Presbyterian promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

200. On information and belief, Presbyterian further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

201. Plaintiff and Class Members paid money to Presbyterian with the reasonable belief and expectation that Presbyterian would use part of its earnings to obtain adequate data security. Presbyterian failed to do so.

202. Plaintiff and Class Members would not have entrusted their Private Information to Presbyterian in the absence of the implied contract between them and Presbyterian to keep their information reasonably secure.

203. Plaintiff and Class Members would not have entrusted their Private Information to Presbyterian in the absence of their implied promise to monitor their computer systems and networks

to ensure that it adopted reasonable data security measures.

204. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

205. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Presbyterian.

206. Presbyterian breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

207. Presbyterian breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of Private Information and storage of other personal information after Presbyterian knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

208. As a direct and proximate result of Presbyterian's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) unconsented disclosure of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed

up in Presbyterian's possession and is subject to further unauthorized disclosures so long as Presbyterian fails to undertake appropriate and adequate measures to protect the Private Information.

209. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT IV
In the Alternative—Unjust Enrichment
(On Behalf of Plaintiff and the Class against Defendant Presbyterian)

210. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

211. The Plaintiff brings this count as an alternative to the breach of implied contract claim (Count III) above.

212. Plaintiff and Class Members conferred a monetary benefit on Presbyterian. Specifically, they paid Presbyterian and/or its agents for the provision of services and in so doing also provided Presbyterian with their Private Information. In exchange, Plaintiff and Class Members should have received from Presbyterian the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

213. Presbyterian knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Presbyterian profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

214. Presbyterian failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

215. Presbyterian acquired the Private Information through inequitable record retention, having failed to investigate and/or disclose the inadequate data security practices previously mentioned.

216. If Plaintiff and Class Members had known that Presbyterian would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information at Presbyterian or obtained services at Presbyterian.

217. Plaintiff and Class Members have no adequate remedy at law.

218. Presbyterian enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Presbyterian instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Presbyterian's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

219. Under the circumstances, it would be unjust for Presbyterian to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

220. As a direct and proximate result of Presbyterian's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) unconsented disclosure of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains

unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Presbyterian's possession and is subject to further unauthorized disclosures so long as Presbyterian fails to undertake appropriate and adequate measures to protect the Private Information.

221. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Presbyterian and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Presbyterian from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

222. Plaintiff and Class Members may not have an adequate remedy at law against Presbyterian, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
Declaratory Judgment
(On Behalf of Plaintiff and the Class against Defendants)

223. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

224. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those here, that are tortious and violate the terms of the federal statutes described in this Consolidated Complaint.

225. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Private

Information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further cyberattacks and data breaches that could compromise their Private Information.

226. Defendants still possess Private Information pertaining to Plaintiff and Class Members, which means their Private Information remains at risk of further breaches due to Defendants' inadequate data security measures. Plaintiff and Class Members continue to suffer injuries resulting from the compromise of their Private Information and remain at imminent risk that additional breaches will occur in the future.

227. Pursuant to the Declaratory Judgment Act, Plaintiff seeks a declaration that: (a) Defendants' existing data security measures fail to comply with their obligations and duties of care; and (b) In order to comply with their obligations and duties of care, Defendants must:

a. Implement policies and procedures to ensure that any parties with whom they share sensitive Private Information maintain reasonable, industry-standard security measures, including, but not limited to, those listed below;

b. Purge, delete, or securely destroy Plaintiff's and Class Members' Private Information if it is no longer necessary for essential business functions, so it is not subject to further theft; and

c. Implement and maintain reasonable, industry-standard security measures, including but not limited to the following: (i) Engaging third-party security auditors/penetration testers and internal security personnel to conduct regular testing, including simulated attacks, penetration tests, and audits on Defendants' systems, and promptly addressing any problems or vulnerabilities detected; (ii) Utilizing automated security monitoring through third-party security auditors and internal personnel; (iii) Auditing, testing, and training security personnel on new or

updated procedures; (iv) Encrypting Private Information and segmenting it with firewalls and access controls to prevent hackers from accessing multiple areas of Defendants' systems in the event of a breach; (v) Purging, deleting, and securely destroying Private Information that is no longer necessary for essential business operations; (vi) Conducting regular database scanning and security checks; (vii) Providing ongoing employee education on best security practices; (viii) Implementing multi-factor authentication and the Principle of Least Privilege (POLP) to combat system-wide cyberattacks; and (ix) Routinely conducting internal training to educate security personnel on breach identification, containment, and response protocols.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grants the following:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members.

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other relief this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: November 22, 2024

Respectfully Submitted,

By: /s/ Norman E. Siegel

Norman E. Siegel (44378MO)
J. Austin Moore (64040MO)
Tanner J. Edwards (68039MO)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
tanner@stuevesiegel.com

Attorneys for Plaintiff and the Proposed Class